

SPLUNK PRIVACY POLICY

Updated: December 2022

This Privacy Policy explains how Splunk Inc. and its subsidiaries ("Splunk") collect, use, and disclose information you provide to us or which we otherwise collect ("Information"), including "Personal Data" by which we mean Information about an identified or reasonably identifiable individual.

This Privacy Policy applies to Offerings (as defined in the [Splunk General Terms](#)), splunk.com and to other websites Splunk operates that link to this Privacy Policy. This Privacy Policy does not apply to Personal Data processed by Splunk as a processor or to Splunk as an employer.

From time to time, Splunk acquires companies that may operate under their own privacy policies. You will continue to be presented with those companies' privacy policies on their offerings and websites until the integration with Splunk is complete and those offerings and websites are linked to this Privacy Policy.

The use of our products and services, including those available through other Splunk websites that link to this Privacy Policy, are subject to the terms of the applicable customer agreement. The use of our website is subject to the [Splunk Websites Terms and Conditions of Use](#). The terms of this Privacy Policy are incorporated into and form part of those agreements.

[Data Collection](#)

[Interactions](#)

[What We Collect via Your Interactions](#)

[How We Use Information Collected from Interactions](#)

[Opting Out of Marketing Emails](#)

[Offerings](#)

[What We Collect via Our Offerings and How We Use It](#)

[Other Collection Practices](#)

[Data Collection Practices Associated with Apps](#)

[How Splunk Shares Your Information](#)

[How We Secure Your Information](#)

[Splunk Also Observes the Following Practices](#)

[Your Rights](#)

[Supplemental Information for Certain Regions](#)

[European Economic Area, the UK and Switzerland](#)

[California & Other US States](#)

[Links to Other Parties](#)

[Updates to This Privacy Policy](#)

[Contact Splunk](#)

[Links to Related Agreements, Policies, and Information](#)

Data Collection

There are two primary ways in which Splunk collects Information about you: through [Interactions](#) and through [Offerings](#) as set forth below.

Interactions

When you interact online or offline with Splunk, we may receive your Information, including your Personal Data. For example, we receive your Information when you:

- Visit Splunk's websites or offices
- Download materials through our websites
- Provide or update account or contact details through our websites
- Register for, attend, speak at or otherwise participate in Splunk-hosted or sponsored events (such as conferences, promotional events, webcasts, contests, or hackathons)
- Participate in community programs and Splunk-related repositories on third-party open-source platforms
- Communicate with us including by email, phone, text, online chat, or social media
- Provide testimonials or feedback

We collect Information about you from other sources such as public databases, commercial data sources, joint marketing partners, resellers, managed services providers and other partners, social media platforms, industry groups, and conference/event hosts.

We refer collectively to these contacts as "Interactions" and we explain below how we use the Information we collect through them.

What We Collect via Your Interactions

We (or others acting on our behalf) may collect your Information, including your Personal Data, through Interactions. The Personal Data we collect includes such things as:

- Name or alias
- Email address
- Physical address, including country
- Employer
- Industry group participation
- Title / position
- Payment details
- Phone number
- Username / user ID

- IP address
- MAC address (or other device identifiers automatically assigned to your device when you access the internet including browser or device type)
- Images and related metadata (for example, when visiting our offices or attending an event)
- Content of your communications and files you input, upload, or create
- Videos (for example, when you provide a product testimonial)

We collect Personal Data in various ways, such as when you manually key in your Personal Data to our website forms or provide it to us or others from whom we receive marketing leads. From time to time, we offer virtual private networks (VPNs) for attendees at Splunk events or visitors to our offices. If you access a Splunk-provided VPN, we may collect Personal Data from you, such as IP and MAC addresses, when we monitor the VPNs for security or performance.

IP addresses are also collected on an automated basis through your use of the website services using cookies, web beacons, and like technologies. We may infer your location from your IP address. For more on the use of cookies and like technologies, see the [Splunk Cookie Policy](#) and [How We Use Information Collected from Interactions](#).

When you make purchases through our website, we use third-party payment processors to collect credit card or other financial data. Splunk does not store the credit card data you provide, only payment confirmation information.

How We Use Information Collected from Interactions

Splunk uses the Information we collect from your Interactions to deliver services to you in accordance with our terms, to fulfill our contractual and legal obligations, or to pursue legitimate business interests, as described below. Here is a summary of the purposes for which we use your Information, including Personal Data, to:

- Fulfill your orders or respond to your requests for information and other inquiries

For example, to satisfy your requests for website materials such as marketing collateral or white papers, we collect and use your name and email address.

- Operate, enhance, and personalize your experience on our website

We collect Information via cookies and other information-gathering technologies as stated in the [Splunk Cookie Policy](#) to fulfill our legitimate interest in operating our website, making it easy to navigate, and enriching the available content and offering information tailored to your interests. In doing so, we may receive your location Information, which you can disable by configuring the location sharing permissions in your device.

- Issue you Splunk accounts for access to online communities and forums and to enable your participation

When you join our online communities and forums, including blogs and Splunk-branded business communication and streaming platform channels (collectively, “Online Forums”), we collect your Personal Data to enable your access and provide an interactive experience when you participate. The guidelines associated with those Online Forums recommend not sharing private or proprietary

Information on them, as many of their aspects are public. If you choose to submit content to online forums, such content will be considered public and will not be subject to the privacy protections set forth in this Privacy Policy except as required by applicable law. Online Forums that display the Splunk name but present you with their own privacy notice are subject to such privacy notice and not this Privacy Policy.

- Send you administrative notices

We may need to notify you (or we may choose to inform you) when we make updates to our terms or policies or make changes to our website or Offerings. We will use your name and email address to send such administrative notices to you, which due to their nature are treated differently from marketing communications from which you can opt out.

- Manage your Splunk account

To perform the services under the contract between you and Splunk, we need to collect certain Information from you such as your contact and payment details. Without this Information, we may not be able to deliver the services or comply with our contractual or legal obligations.

- Advertise and market to you

With your consent or to pursue legitimate business interests, we may contact you with announcements about our Offerings, educational materials, announcements about special offers, or Information about upcoming or ongoing online/offline events, such as .conf, and related offers. If required by applicable law, we will ask you for your consent before sending and/or give you the choice to [opt out](#) of receiving these communications.

- Administer prize promotions and events

We use your Information to administer prize promotions and events based on the terms of the promotion or event. For example, if you enter into a prize promotion, we may use your data to select a winner and provide the prize to you if you win. Or, if you register for a coding workshop or a gaming or other event, we may add your name to the list of expected attendees. If you win, we may seek your consent to announce you as a winner, which you may withdraw at any time. However, we will retain Information collected in connection with your enrollment with the prize promotion or event.

- Invite you to participate on customer advisory boards or in surveys, studies, and assessments of Offerings

We use your Personal Data to register you to participate on advisory boards (such as our Customer Advisory Boards, Product Advisory Councils, or Developer Advisory Boards) or to request feedback from you about our Offerings. We use your feedback to fulfill our legitimate interest in improving our Offerings and growing our business. Your participation is voluntary and subject to the terms of your agreements with us and this Privacy Policy.

- Diagnose and fix technical issues, monitor for security, and otherwise protect our property

We do this to satisfy our legitimate interest in assessing actual or potential technical issues or threats to our facilities, attendees at Splunk-sponsored events, our IT systems and networks, Offerings, and website services. We may process your Information, in particular your IP address, for this purpose.

- Comply with law

We may use your Information to comply with any applicable laws, regulations, legal process+, or governmental requests, or to protect our legal rights or those of others.

- For any other purpose disclosed to you in connection with our Offerings, website services, or other third-party platforms from time to time

If we process your Personal Data for other purposes, we will provide you with information about such processing, and if required, obtain your consent.

Opting Out of Marketing Emails

If you no longer want to receive marketing emails from Splunk on a go-forward basis, please submit your request through our online [opt-out form](#). Alternatively, you may use the "unsubscribe" feature in our marketing email messages to opt-out of receiving marketing email messages.

Offerings

We also collect Information, including Personal Data, when providing our Offerings. We may ask you for this Information directly, or in some cases, we may collect it as you use our Offerings. For example, we collect Information from or about you when you (or someone you work with):

- Order or sign up for a trial of our Offerings
- Interact with Splunk online or offline, including when you request support services
- Use our Offerings

What We Collect via Our Offerings and How We Use It

We collect and process different types of data (described below) when you deploy our Offerings in order to fulfill our contractual and legal obligations and operate our business or fulfill other legitimate interests. We summarize for you here the types of data collected and the purposes for which we use this data, which may include your Information:

Usage Data is data about your operating environment and configuration, user interactions, and sessions related to your use of our Offerings. This may include information and related metadata about your network and systems architecture and configurations, OS and Offering versions, Offering configurations, installed applications, feature utilizations and frequencies, page loads and views, number and types of searches, errors, number of active and licensed users, source, source types and formats (e.g., json, xml, and csv), web browser details, http referrer page, and app workflows.

- **License Usage Data** is data that allows us to identify account entitlements, such as license entitlement consumption, license capacity, or license type in our systems through an assigned license ID. We use this data to validate accounts, automate license verification, and offer enhancements.

- **Support Usage Data** is Usage Data coupled with License Usage Data that offers you accelerated troubleshooting, notices of patches/upgrades, tips to optimize usage, security, configurations and/or performance, and suggestions about other Offerings that may be of interest to you. The Information is user/customer-identifiable so that we can help address your specific issue and personalize your experience. From time to time, we may also use the information to analyze usage trends, such as by data type, environment size, scale and architecture, and industry or sector, to develop and prioritize product enhancements (e.g., bug fixes or new features).
- **Mobile Device Data** is data we collect in certain Offerings (“Apps” as discussed below) that associates your mobile device with an identifier for your App to help us improve the user experience and personalize your services and content. We may also receive information that your mobile device sends when you use our Apps, such as a device identifier or OS. Depending on a customer’s configuration of our Offerings, location information about users may be shared with Splunk. You can disable location sharing using the location-setting features on your mobile device.
- **Security Offerings Data.** Certain security-focused Offerings collect, and in some cases allow, sharing of Customer-submitted “artifacts” (such as logs, alerts, emails, cases, and incidents) and intelligence sources to support security investigation, threat detection and monitoring. In some cases, this information may contain names, IP addresses, email addresses, phone numbers and other types of Personal Data contained in such artifacts and intelligence sources. You determine the extent and nature of the data you submit and whether to participate in such Offerings and in some cases to share the data with Splunk.

Certain Offerings rely on automated methods of processing, such as artificial intelligence and machine learning, which is a set of technologies and processes that allow computers to learn, adapt, predict, and assist in decision making. These technologies may consume data or other Information that may be associated with you. The use of data in connection with such Offerings is set forth in the relevant terms.

For more information about the data and Information collected through our Offerings, see [the Offering-specific documentation](#) (e.g., [Share data in Splunk Enterprise](#) in the Splunk Enterprise Admin Manual).

We use the data and Information described above to fulfill our contractual obligations in providing the Offerings to you and to fulfill our legitimate interest in supporting and enhancing them. For example, we may use this data and Information to:

- Troubleshoot issues, provide support, and update our Offerings
- Provide guidance to help you optimize your configuration, security, and usage of our Offerings
- Better understand how our users use and configure our Offerings
- Determine which configurations or practices optimize performance (e.g., best practices)

- Benchmark key performance indicators (“KPIs”)
- Recommend enhancements
- Perform data analysis and audits
- Identify, understand, and anticipate performance issues and the factors that affect them
- Identify product security issues that may affect you and inform you of them
- Improve and develop new features and functionality
- Monitor the health, performance, and security of our Offerings

In our paid on-premises products, the level of participation can be selected and changed. For more details on what we collect and participation options, see [Splunk's Documentation](#).

Other Collection Practices

We also collect Information from you to fulfill our contractual commitments to you. For example, we collect contact Information such as name, address (email and physical) and phone number to enter you into our databases and manage your account. We also collect billing and payment Information and information about how you use our Offerings, including Information such as browser type, version number and OS, to administer your account, respond to customer service/support inquiries, and provide you with information about software updates via alerts or other “push” notifications. We may share this Information as described in [How Splunk Shares Your Information](#). We do not sell this Information.

Data Collection Practices Associated with Apps

Splunk’s Offerings are extendible using software applications commonly called “apps,” “add-ons,” “widgets,” or “technical add-ons” that we offer through splunkbase.splunk.com or other websites that may link to this Privacy Policy. We refer to these collectively as “Apps.” These Apps are versatile and have access to a broad set of web technologies that can be used to collect and use your Information. This Privacy Policy only applies to Apps built by or on behalf of Splunk. It does not apply to Apps developed by others (“App Developers”), including those built by Splunk Works and Splunk Labs, which may be available through splunkbase.splunk.com, third-party marketplaces or repositories (e.g., AWS Marketplace, Google Play Store, and GitHub), or that are otherwise interoperable with our Offerings.

Splunk requires App Developers to comply with applicable privacy and data protection laws but cannot guarantee that they do so. Before you use Apps created by App Developers, you should familiarize yourself with their privacy policies and license agreements.

Splunk collects Information generated from the use and performance of Apps that interoperate with its Offerings, such as crash data, version, session duration, and user engagement (e.g., number of downloads, active/licensed users, and logins). We may share this data with App Developers so they can improve and enhance the performance of their Apps.

How Splunk Shares Your Information

Splunk may disclose your Information to others in the following ways:

- **Subsidiaries.** We may disclose Information to our [subsidiaries](#) subject to this Privacy Policy so that they can help market, sell, and service our Offerings. Splunk is the party responsible for the management of jointly used Personal Data. Splunk maintains intragroup agreements covering the use of Personal Data within the Splunk family of companies.
- **Service Providers.** We may disclose Information to our service providers (e.g., infrastructure as a service, order fulfillment, professional/customer/support services), pursuant to written agreements with confidentiality, privacy, and security obligations.
- **App Developers.** We may disclose Information about App use and performance with App Developers so that they can improve and enhance the performance of their Apps. With your consent, we may also disclose your Information to App Developers to help support the performance of their Apps. App Developers will be identified to you when you download and use their Apps pursuant to their license and other terms.
- **Partners and Sponsors.** We may disclose account and contact details to our [partners](#) and event hosts/sponsors (identified at time of registration or event participation) pursuant to written agreements with confidentiality, privacy, and security obligations. They may use the Information to assess your interest in our Offerings, conduct user research and surveys, or send you marketing communications, subject to the terms of their privacy policies. We may also share Support Usage Data with partners when they manage your Offering for you.
- **Internet Activity Service Providers.** As described further in the Splunk Cookie Policy, we may disclose internet or other electronic network activity Information, including, but not limited to, browsing history, search history, and Information regarding a consumer's interaction with a website, or advertisement if you accept advertising and social media cookies.
- **Online Forums.** When you take certain actions on blogs and Splunk-branded business communication and streaming platform channels ("Online Forums") that are public or intended to be public in nature, such as when you broadcast content, participate in a chat room, post profile Information, or follow a channel, that Information may be collected, used, or disclosed by other participants in the Online Forums. In addition, some features of Online Forums are designed to provide others with Information about user activity, such as the subscription status of users for a given channel.
- **Compliance and Safety.** We may disclose Information as necessary or appropriate under applicable laws (including laws outside your country of residence) to: comply with legal process or requirements; respond to requests from public or government authorities (including those outside your country of residence); enforce our terms and conditions; and protect our operations and rights and safety of you and others, as needed. For more information about data we disclose in response to requests from law enforcement and other government agencies, please see the Splunk [Data Request Guidelines](#).
- **Merger, Sale, etc.** We may disclose Information in the event of a proposed or actual corporate or financing transaction, such as a reorganization, merger, sale, joint venture, assignment, transfer, or

disposition of all or any portion of Splunk business, assets, or stock (including Information regarding any bankruptcy or similar proceedings).

- **Other Users.** We may disclose Information to other users of the service in aggregated format, provided it does not include Personal Data. This may include “best practices” tips, KPIs, benchmarking data or other such aggregated Information useful to the user community. For select Offerings, we may share Information you provide, such as security artifacts that may contain Personal Data (e.g., IP address) with other subscribers, but only if required as part of the Offering, as set forth in the relevant terms.

How We Secure Your Information

Splunk takes reasonable technical and organizational measures to safeguard Personal Data against loss, theft, and unauthorized access, disclosure, alteration, misuse, or destruction. Unfortunately, no data transmission, software, or storage system can be guaranteed to be 100% secure. If you have reason to believe that your Personal Data may no longer be secure (for example, if you feel that the security of an account has been compromised), please notify us immediately via the communication channels in the [Contact Splunk](#) section below. If Splunk learns of a breach of its systems, Splunk may notify you or others consistent with applicable law and/or as agreed in our contract with you. Splunk may communicate with you electronically regarding privacy and security issues affecting Information collected through your Interactions or use of our Offerings.

Splunk Also Observes the Following Practices

Retention Period. We retain your Information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or not prohibited by applicable law. Information you store in Splunk cloud environments is portable by you at the end of the term of your agreement with Splunk. We retain your contract Information for the duration of your agreement with us and thereafter as required or permitted by law. We keep a record of your data requests, including your requests to opt out of marketing communications, to honor them in the future. See the [Splunk Data Retention Policy](#) for additional details.

Use of Offerings by Minors. Our Offerings, splunk.com and other websites Splunk operates are not directed to individuals 16 and under or those not of the age of majority in your jurisdiction, and we request that these individuals, or others on their behalf, not provide us with their Information.

Your Rights

In certain locations, you may have rights under data protection law, such as to request access to or correction, deletion, or transfer of your Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our [data request form](#), and we will respond as soon as reasonably practicable consistent with applicable law. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

Supplemental Information for Certain Regions

European Economic Area, the UK and Switzerland

We rely on a variety of legal bases to process Personal Data, including your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with a legal obligation. If we process your Personal Data based on your consent, you may withdraw your consent at any time. We will let you know if we are seeking to rely on your consent at the time of collection.

In Europe, Splunk Services UK Limited co-controls Personal Data required for contracts and accounts as described above in [Offerings](#) and [Other Collection Practices](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under Contact Splunk below. If your request or concern is not satisfactorily resolved by us, you can approach your local data protection authority. You can find your local data protection authority in the EU [here](#), in the UK [here](#), and in Switzerland [here](#).

Your Rights

Individuals located in the UK, Switzerland or European Economic Area are granted certain rights related to Personal Data, including the ability to:

- Ask whether we process Personal Data about you, and if we do, to access the Personal Data and certain information about how we use it and who we share it with;
- Request that we delete the Personal Data we hold about you in certain limited circumstances;
- Request that we stop processing the Personal Data we hold about you;
- Request that your Personal Data be provided to you or another organization in a structured, commonly used and machine-readable format;
- Object to our processing of data about you, including in relation to processing your Personal Data for marketing purposes; and
- Withdraw consent if processing of your Personal Data is based on consent.

If you or a designated third-party agent would like to exercise these rights, please submit the request through our data request form, and we will respond in accordance with our legal obligations. We will verify your identity, and the identity of any third-party agent acting on your behalf, before we comply with the request and ask for your cooperation with our identity verification process.

Lawful Basis for Transferring Your Data: Cross-border Transfers

Your Personal Data may be stored and processed in any country where Splunk, its subsidiaries, partners, sub-processors, and third-party service providers conduct business or host events. These locations may be outside of your country of residence, including in the United States, where different data protection laws may apply. When we transfer Personal Data, we implement safeguards for protection of the transferred Personal Data, such as standard contractual clauses. We put in place appropriate terms to protect your Personal Data in our agreements with our service providers, processors, and sub-processors.

Privacy Shield

Splunk has certified to the Department of Commerce that we adhere to the Privacy Shield Principles (“Principles”) of the EU-U.S. and Swiss-U.S. Privacy Shield frameworks, as further described in the Splunk Privacy Shield Notice, although Splunk does not rely on the frameworks as a legal basis for transfers of Personal Data. If there is any conflict between the terms in this Privacy Policy and the Principles, the Principles will govern. To learn more about the Privacy Shield program, please visit privacysshield.gov, where you can view Splunk’s certifications.

California & Other US States

California

Capitalized terms in this section are as defined in the California Civil Code.

If you are a California Consumer, California law provides you with specific rights regarding your Personal Information, subject to certain exceptions. These rights include:

- the right to know the categories of Personal Information a business collects about you, the purposes for which such Information is collected or used, whether the Information is sold or shared, and the length of time a business intends to keep the Information;
- the right to request deletion of your Personal Information a business collects from you;
- the right to request correction of inaccurate Personal Information;
- the right to request disclosure of Information collected, including specific pieces of Personal Information collected about you;
- the right to request disclosure of Information Sold or Shared;
- the right to opt-out of the Sale or Sharing of Personal Information; and
- the right to non-discrimination for exercising your rights.

If you or a designated third-party agent would like to exercise these rights, please submit the request through our [data request form](#) or via our toll-free number XXX-XXX-XXXX, and we will respond in accordance with our legal obligations. We will verify your identity, and the identity of any third-party agent acting on your behalf, before we comply with the request and ask for your cooperation with our identity verification process.

Splunk may collect the following categories of Personal Information from California Consumers for purposes outlined in [How We Use Information Collected from Interactions](#) and [What We Collect via Our Offerings and How We Use It](#):

- Identifiers or other elements of Personal Information under California Civil Code Section 1798.80 and 1798.140 such as those described in [What We Collect via Your Interactions](#). Identifiers are retained for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or not prohibited by applicable law.
- Characteristics of protected class Information about veteran’s status if you applied for a veteran’s discount on educational credits. Splunk does not collect this Information directly. We use

service providers to confirm eligibility. Eligibility status is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or not prohibited by applicable law.

- Characteristics of protected class Information to verify disability status to grant reasonable accommodations for Splunk Certification testing. This Information is not stored by Splunk, only whether an accommodation was granted.
- Commercial Information about products or services as described in [Other Collection Practices](#). This commercial Information is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or not prohibited by applicable law.
- Internet or other electronic network activity when you interact with Splunk's website as described in [What We Collect via Your Interactions](#), [What We Collect via Our Offerings and How We Use It](#), and the [Splunk Cookie Policy](#). Internet or other electronic network activity data is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the Splunk Cookie Policy unless a longer retention period is required or not prohibited by applicable law. This Information may be Shared if you accept advertising and social media cookies. If you do not opt-in, this Information will not be Shared. You may change your cookie preferences at any time via the [Splunk Cookie Policy](#). The categories of third parties that receive this cookie data are outlined in Splunk's cookie banner and [Splunk Cookie Policy](#). A full list of cookies and their sources are identified on [Splunk's Cookie Appendix](#).
- Geolocation data such as IP address as described in [What We Collect via Your Interactions](#), [What We Collect via Our Offerings and How We Use It](#), and the [Splunk Cookie Policy](#). Geolocation data is retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the [Splunk Cookie Policy](#) unless a longer retention period is required or not prohibited by applicable law. This Information may be Shared if you accept advertising and social media cookies. If you do not opt-in, this Information will not be Shared. You may change your cookie preferences at any time via the [Splunk Cookie Policy](#). The categories of third parties that receive this cookie data are outlined in Splunk's cookie banner and the [Splunk Cookie Policy](#). A full list of cookies and their sources are identified on [Splunk's Cookie Appendix](#).
- Inferences drawn from any of the Information identified in 1798.140. Any such inferences will be retained for the period necessary to fulfill the purposes outlined in this Privacy Policy and within the [Splunk Cookie Policy](#) unless a longer retention period is required or not prohibited by applicable law.

Within the scope of this Policy, Splunk does not collect or process Sensitive Personal Information about California Consumers.

Splunk did not – in the preceding 12 months – and does not Sell or Share Personal Information of California consumers.

The source of each of these categories of Personal Information are outlined in this Privacy Policy in the Interactions and Offerings sections respectively.

The categories of Third Parties to whom Personal Information may be disclosed are outlined in this Privacy Policy in the [How Splunk Shares your Information](#) section. We may have disclosed any of the above categories of Personal Information pursuant to an individual's consent or under a written contract with a Service Provider for a Business Purpose.

Colorado

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above.

Consumers in Colorado have rights under data protection law, such as to request access to or correction, deletion, or transfer of their Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you, or a person you have authorized, would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our [data request form](#), and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

In the event Splunk declines to take action on your request, we will inform you via our response to your request of your right to appeal the decisions with instructions for how to submit your appeal. Once an appeal is received, Splunk will respond to the appeal with details on any action taken and reasons supporting our decision within forty-five (45) days.

Splunk does not sell your Personal Data (as defined by Colorado law). To opt-out of targeted advertising, ensure you opt-out of Advertising and Social Media cookies via Splunk's cookie banner or via the [Splunk Cookie Policy](#). Additional details are available via the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Connecticut

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above.

Consumers in Connecticut have rights under data protection law, such as to request access to or correction, deletion, or transfer of their Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you, or an authorized agent you designate, would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our data request form,

and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

In the event Splunk declines to take action on your request, we will inform you via our response to your request of your right to appeal the decisions with instructions for how to submit your appeal. Once an appeal is received, Splunk will respond to the appeal with details on any action taken and reasons supporting our decision within sixty (60) days.

Splunk does not sell your Personal Data (as defined by Connecticut law). To opt-out of targeted advertising, ensure you opt-out of Advertising and Social Media cookies via Splunk's cookie banner or via the [Splunk Cookie Policy](#). Additional details are available via the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Nevada

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above. To the extent material changes are made to this Privacy Policy, you will be informed via the process outlined in the Updates to this Privacy Policy section.

Consumers in Nevada have rights under data protection law, such as to request updates to certain Personal Data elements considered "Covered Information" under Nevada law. If you would like to exercise your rights, please submit your request, with a description of the nature of your request and the Covered Information at issue, through our data request form, and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

Covered Information under Nevada law may be collected over time and across different websites if your browser enables cookies. To prevent this, ensure you opt-out of Advertising and Social Media cookies via Splunk's cookie banner or via the [Splunk Cookie Policy](#). Additional details are available via the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Utah

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above.

Consumers in Utah have rights under data protection law, such as to request access to or correction, deletion, or transfer of their Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our data request form, and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

Splunk does not sell your Personal Data (as defined under Utah law). To opt-out of targeted advertising, ensure you opt-out of Advertising and Social Media cookies via Splunk's cookie banner or via the [Splunk Cookie Policy](#). Additional details are available via the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Virginia

The categories of Personal Data processed, the purposes of processing Personal Data, the categories of Personal Data shared with third parties and the categories of third parties with whom Splunk shares Personal Data are as outlined above.

Consumers in Virginia have rights under data protection law, such as to request access to or correction, deletion, or transfer of their Personal Data, or to object to or restrict Splunk from using it for certain purposes. If you would like to exercise these rights, please submit your request, with a description of the nature of your request and the Personal Data at issue, through our data request form, and we will respond in accordance with our legal obligations. We will verify your identity before we comply with your request and ask for your cooperation with our identity verification process.

In the event Splunk declines to take action on your request, we will inform you via our response to your request of your right to appeal the decisions with instructions for how to submit your appeal. Once an appeal is received, Splunk will respond to the appeal with details on any action taken and reasons supporting our decision within sixty (60) days.

Splunk does not sell your Personal Data (as defined by Virginia law). To opt-out of targeted advertising, ensure you opt-out of Advertising and Social Media cookies via Splunk's cookie banner or via the [Splunk Cookie Policy](#). Additional details are available via the [Splunk Cookie Policy](#).

If you have any questions or concerns about Splunk's privacy practices, you can contact us at any time via the contact options listed under [Contact Splunk](#) below.

Links to Other Parties

Our Offerings may contain links to, or facilitate access to, other websites or online services. This Privacy Policy does not address, and Splunk is not responsible for, the privacy, information, or practices of other parties, including without limitation any App Developer, social media platform provider, wireless service provider, or device manufacturer. The inclusion of a link within the Offerings does not imply endorsement of the linked site or service by Splunk. Splunk encourages you to review the privacy policies and learn about the privacy practices of the companies whose websites you choose to visit or Apps you choose to use. We list below links to resources about many of the other parties with whom we interact as described in this Privacy Policy:

- For [partners](#)
- For App Developers listed on [Splunkbase](#)
- For other marketplaces where Splunk Apps may be found
- For [industry content providers](#) (such as providers of research, white papers, etc.)
- For [industry award providers](#) (such as those listed on Splunk.com)
- For other resources (such as source code repositories, sample data sources, customers, etc.) mentioned in [blogs and press releases](#)
- For other providers, sponsors, or speakers at [events](#) in which Splunk is involved
- For social media platform providers (such as [Twitter](#), [GitHub](#), [Twitch](#), [LinkedIn](#), [YouTube](#), or [Facebook](#))

Updates to this Privacy Policy

We may change this Privacy Policy from time to time and will post our updates [here](#). We will also communicate any material changes of the Privacy Policy to you.

Contact Splunk

If you have any questions or comments about this Privacy Policy or Splunk's privacy practices, you can contact us at any time at dpo@splunk.com or by mail as provided below:

Splunk Inc. Office of the Data Protection Officer 270 Brannan Street San Francisco, CA 94107	Splunk Services UK Limited Office of the Data Protection Officer Brunel Building 1 & 2 Canalside Walk London W2 1DG England	Splunk Services Germany GmbH Office of the Data Protection Officer Mies-van-der-Rohe-Straße 6 80807 München Germany
-------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------